IN THE CLAIMS:

Please cancel claims 1 – 26 in their entirety and without prejudice and substitute the following new claims:

--27. A method for protecting one or more computer systems using the same secret key (Ks) cryptographic algorithm, characterized in that secret data (Ds) stored in a secret area of the computer system or systems is utilized to perform a cryptographic calculation for each computer system and for each secret key.

28. The method according to claim 27, characterized in that, for each computer system and for each secret key (Ks), the way in which said secret data (Ds) is used to perform said cryptographic calculation is public.

29. The method according to claim 27, characterized in that in each of the computer systems, each secret key (Ks) used by said cryptographic calculation corresponds to a specific piece of said secret data (Ds).

30. A method according to claim 27 for protecting one or more computer systems wherein the cryptographic calculation uses nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address that is a function of the km input bits, and for each of said nonlinear transformations, said k tables are part of the secret data (Ds).

31. A method according to claim 27 for protecting one or more computer systems wherein the cryptographic calculation process uses nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address obtained by applying a secret bijective function (φ) to an m-bit value, itself obtained by applying a public function of the km input bits of the nonlinear transformation, and for each of said nonlinear transformations, said k tables are part of the secret data (Ds).

32. The method according to claim 27, comprising storing a conversion table calculation program in each computer system and activating the calculation program by a given event in order to calculate tables and store all or part of said tables in the secret data (Ds)..

33. A computer system comprising storage means for storing a modified cryptographic algorithm that adheres to computational phases of astandard cryptographic algorithm, a secret encryption key contained in a secret area of the storage means for modifying the standard cryptographic algorithm, means for executing saud modified cryptographic algorithm, first secret means for replacing intermediate variables required for the computational phases of the standard algorithm with a plurality (k) of partial intermediate variables, second means for applying a nonlinear transformation table to each of said partial intermediate variables, and third secret means for reconstituting a final result corresponding to utilization of the standard cryptographic algorithm from results obtained on the partial variables.

34. A computer system according to claim 33, characterized in that secret encryption key stored in the secret area includes at least one first random variable v_1 constituting at least one secret partial variable, and the modified cryptographic algorithm determines at least one other partial variable v_2, by applying a first secret function to the intermediate variable v and the secret partial variable or variables v_1.

35. A computer system according to claim 34, characterized in that the modified cryptographic algorithm includes tables used for applying the nonlinear transformations to the partial variables v_1 and v_2, at least one of said tables (A), formed by random selection, and being stored in the secret data Ds, the other tables required for the calculations being stored in a nonvolatile memory, means for executing various computational rounds of the standard algorithm, each time using the tables on the partial variables, and means for calculating the result in the last round of the algorithm by combining the partial variables in accordance with a second secret function.

36. A computer system according to claim 33, characterized in that the first secret means of the modified algorithm are constituted by a function *f*, linking the partial intermediate variables and each intermediate variable (*v*), such that the knowledge of one value of said intermediate variable never makes it possible to deduce all of the particular partial values v_i such that there exists a *(k-1)-tuple* $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots v_k)$ that satisfies the equation $f(v_1, \ldots, v_i, \ldots, v_k) = v$.

37. A computer system according to claim 33, characterized in that the second means of the modified algorithm are constituted by k partial conversion tables, and among the *k* partial conversion tables, *k-1* partial conversion tables contain secret random variables.

38. A computer system according to claim 37, characterized in that the second means of the modified algorithm comprise k conversion tables, each of said conversion tables receiving an input a value obtained by applying a secret bijective function φ_1 to said function $f(v_1,\ldots, v_k)$ of the partial intermediate variables in accordance with the relation $\varphi_j \circ f(v_1, \ldots,v_k)$, $j \in [1,k]$, this application $\varphi_j \circ f(v_1,\ldots, v_k)$ being performed by direct evaluation of a resulting value, this resulting value, applied to the input of the conversion table, making it possible to read *n* output bits of the transformation at an address that is a function of these *m* input bits.

39. A computer system according to claim 33, characterized in that the second means of the modified algorithm comprise means for replacing each nonlinear transformation applied to an intermediate variable of the standard cryptographic calculation process, without a separation, with a partial nonlinear transformation of *km* bits into *kn* bits applied to all of the partial intermediate variables, means for calculating *(k-)n* of said output bits of this transformation as a polynomial function of the *km* input bits, and means for reading the remaining *n* bits of said output bits by reading a conversion table in which the *n* remaining bits are read at an address that is a function of the *km* input bits.

40. A computer system according to claim 33, characterized in that it

further includes means for sequentially executing operations performed by the modified algorithm in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

41. A computer system according to claim 33, characterized in that it includes means for executing, in interleaved fashion, operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

42. A computer system according to claim 33, characterized in that it includes means for simultaneously executing operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts, in the event of multiprogramming.

43. A computer system according to claim 33, characterized in that it includes means for simultaneously executing, in different processors working in parallel, the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

44. A computer system according to claim 33, characterized in that it includes a conversion table calculation program stored in each computer system and means for activation by a given event of the calculation of the tables and for the storage of all or part of these tables in the secret data.

45. A computer system according to claim 33, further including a counter having means for storing a value that is incremented with each cryptographic calculation so as to constitute a given event for the activation, by activating means, of the calculation of the tables when a given value is exceeded.--